UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,142	12/27/2000	Thomas Wille	DE000002	4761

65913 7590 02/27/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
02/27/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	09/749,142	WILLE ET AL.	
	Examiner	Art Unit	
	MINH DINH	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4, 6-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,4 and 7-14* is/are rejected.

7)☒ Claim(s) *3 and 6* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Art Unit: 2132

DETAILED ACTION

Response to Amendment

1. This Office Action is in response to the RCE/amendment filed 03/12/07. Claims 15-28 have been cancelled.

Response to Arguments

2. Applicant's arguments filed 03/12/07 have been fully considered but they are not persuasive. Applicant argues that executing the dummy operation of Jahnich (6,725,374) simultaneously with a useful operation would be directly contrary to Jahnich's specific teaching that useful and dummy operations should be randomly distributed overtime (page 6, first full paragrah). Jahnich teaches that executing of dummy operations causes additional advantageous current fluctuations to be observed in a DPA analysis and thus contributes to the confusion of an attacker (col. 6, lines 28-37). Jahnich further teaches that it would provide additional benefits if the dummy operations are randomly distributed over time, i.e., they are not executed in a fixed order in relation to the useful operations (col. 6, lines 39-48). Because the dummy operations are not executed in a fix order, it does not mean that they cannot be executed simultaneously with useful operations. A well known problem in parallel processing art is that two operations may not be simlultaneously executed if execution of one

operation depends on the result of execution of the other, i.e., one has to wait for the other to finish. However, Jhanich's dummy operations do not influence the useful operations, and, therefore, are prime candidates for parallel processing. The combination of Patarin and Jahnich would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2, 4, 7, 9 and 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin et al. (6,658,569) in view of Jahnich et al. (6,725,374).

Regarding claims 2 and 10, Patarin discloses a device comprising a central processing unit and one or more co-processors for performing cryptographic operations simultaneously and in parallel (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40). Patarin does not teach the use of dummy operations when performing a cryptographic operation. Jahnich

discloses using dummy operations, whose execution does not influence an encryption result and that the consumption characteristics generated by the dummy operation is part of the consumption characteristics of the smart card when executing the cryptographic operation and the dummy operation so that reconstruction of the consumption characteristics associated with performing the cryptographic operation is impeded (col. 6, lines 29-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Patarin to use dummy operations when performing a cryptographic operation, as taught by Jahnich, so that reconstruction of the consumption characteristics associated with performing the cryptographic operation would be impeded. Accordingly, the dummy operation is performed in parallel and simultaneously with the cryptography operations.

Regarding claims 4, 7, 11-13, Patarin further discloses that the cryptographic operation is split up into at least two sub-operations and at least two processors perform the sub-operations in parallel and simultaneously, while subsequently corresponding sub-results are combined to an overall result of the overall cryptographic operation (Fig. 2; col. 12, lines 6-12 and 31-40).

Regarding claim 9, Patarin further discloses that the sub-operations are parts of an encryption in accordance with DES (figures 3a-b).

5. Claims 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Jahnich as applied to claims 7 and 13 above, and further in view of Tan (6,490,353). Patarin and Jahnich do not disclose that the split-up of the cryptographic operation is randomly controlled. Tan discloses that data to be encrypted is segmented into blocks and that the size of each data block and length of the corresponding encryption key for each block are randomly selected (col. 3, lines 8-42); the selection of the block size and the key length meet the limitation of splitting up a cryptographic operation. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the split-up of the cryptographic operation is randomly controlled, as taught by Tan, to increase the degree of difficulty in attacking the encryption system.

Allowable Subject Matter

6. Claims 3 and 6 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MINH DINH whose telephone

number is (571)272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. D./
Examiner, Art Unit 2132

02/19/08

Art Unit: 2132

/Benjamin E Lanier/

Primary Examiner, Art Unit 2132